REMARKS

I. Claim Rejections - 35 USC §112

The Examiner rejected claims 26-31 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

Regarding claim 26, the Examiner argued that the phrase "transmitting an RF signal containing an authentication code from a first type of access device and a second type of access device" is confusing and unclear. The Examiner argued that it is not understood what is meant by such a limitation. The Examiner asked is the RF signal the same/identical RF signal? The Examiner asked is only one authentication code of the first type of access device and the second type of access device transmits another RF signal containing another authentication code and different than the authentication code and different than the authentication code of the first type of access device.

The Examiner rejected claims 27-31 as being dependent upon a rejected claim 26 above.

The Applicant notes that claims 26-31 have been cancelled via the amendments presented herein, thereby rendering moot the Examiner's argument with respect to these claims.

II. Claim Rejections - 35 USC §102

Requirements for Prima Facie Anticipation

A general definition of *prima facie* unpatentability is provided at 37 C.F.R. §1.56(b)(2)(ii):

> A *prima facie* case of unpatentability is established when the information *compels a conclusion* that a claim is unpatentable under the preponderance

> of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability. (*emphasis added*)

"Anticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W.L. Gore & Associates v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303, 313 (Fed. Cir. 1983) (citing *Soundscriber Corp. v. United States*, 360 F.2d 954, 960, 148 USPQ 298, 301 (Ct. Cl.), *adopted*, 149 USPQ 640 (Ct. Cl. 1966)), *cert. denied*, 469 U.S. 851 (1984). Thus, to anticipate the applicants' claims, the reference cited by the Examiner must disclose each element recited therein. "There must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention." *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 18 USPQ 2d 1001, 1010 (Fed. Cir. 1991).

To overcome the anticipation rejection, the applicants need only demonstrate that not all elements of a *prima facie* case of anticipation have been met, *i.e.*, show that the reference cited by the Examiner fails to disclose every element in each of the applicants' claims. "If the examination at the initial state does not produce a prima face case of unpatentability, then without more the applicant is entitled to grant of the patent." *In re Oetiker*, 977 F.2d 1443, 24 USPQ 2d 1443, 1444 (Fed. Cir. 1992).

Ritter

The Examiner rejected claims 38-39 and 46-47 under 35 U.S.C. §102(e) as being anticipated by Ritter (U.S. Patent Application No. 7,084,736).

Regarding claims 38 and 46, the Examiner argued Ritter discloses a method and an access control system (citing Ritter col. 2, lines 12-23; and FIGS. 1-3), comprising: an authorization-checking device 90 (i.e. an access device) (citing Ritter col. 3, lines 15-23; col. 4, lines 35-44; and FIG. 1); and an identification module 40 and a contactless interface 41 (i.e. a plurality of authorization modules) in association with said authorization-checking device 90 (i.e. access device) (citing Ritter col. 3, lines 23-36; col. 4, lines 1-12; and FIGS. 1 to 3), and both identification module 40 and a contactless interface 41 utilizing the same RF protocol (citing Ritter col. 4, lines 14-22); wherein the identification module includes identification data which comprises a fingerprint and other biometric parameters that can be determined whether the user of the identification module is also the rightful owner (citing Ritter col. 3, lines 38-51; FIG. 1) (i.e., the Examiner argued that at least one of said plurality of authorization modules receives fingerprint data from a user in order to authorize said user to utilize said access device, wherein said fingerprint data is processed by said at least one of said plurality of authorization modules) and wherein the contactless interface 41 includes authorization data (i.e. the Examiner argued that at least one other of said plurality of authorization modules receives an authorization code from a memory location) (citing Ritter col. 4, lines 13-17; col. 5, lines 29-38).

The Applicant respectfully disagrees with this assessment and notes that the Examiner has cited Ritter for disclosing the plurality of authorization modules, citing identification module 40 and a contactless interface 41. The Applicant intended to include the limitation of a plurality of authorization modules as part of the *access control system* implemented as a software or hardware module of the processor, <u>not</u> part of the badge and/or keyfob. The Examiner has cited the plurality of authorization as items 40 and 41 (FIG. 1 of Ritter) which are part of the *authorization badge* and not the access system. The Applicant has amended claims 38 and 46 to clarify the claims with the limitation wherein the plurality of authorization modules is <u>executed by a processor</u>. This limitation was in claims 39 and 47 and has been moved to the independent claims. Ritter does <u>not</u> disclose this limitation as Ritter does not disclose a plurality of authorization modules executed by a processor.

The Applicant further notes that claims 38 and 46 have been amended to include the limitation of a processor, which is adapted to determine which of the plurality of authorization modules is to be executed. This is disclosed in Applicant's paragraph [0025] and in Applicant's FIG. 4 as indicated by step 64. The Applicant's invention is an access device which utilizes *either* a high security keyfob or a lower security badge. The access device may utilize *either* but must make a *determination* of which access authorization device is utilized and thereafter execute the appropriate authorization module.

Ritter does not disclose this limitation. Ritter utilizes *both* identification data and authorization data (i.e. high security keyfob only) as disclosed in Ritter col. 3, lines 38-51, as follows:

> "*Identification data and authorization data of the user are stored in various storage areas in the identification module.* The user's identification data comprise preferably the user's identity, for example his name and/or user number. If the identification module 40 can also be used as SIM (Subscriber Identification Module) card in a mobile telephone, the user's identity can also consist of his IMSI (International Mobile Subscriber Identification) number in the mobile radio network. In a variant embodiment, the identification data comprise also biometric parameters of the user, for example a photograph, voice parameters, iris and/or retina parameters, a finger print etc. With these biometric parameters, it can be reliably determined whether the user of the identification module is also the rightful owner." (emphasis added)

Ritter therefore discloses only *one* type of authorization device (i.e. similar to a keyfob). With only one type of authorization *device* disclosed, only one type of authorization *module* (as part of the processor of the access system) is necessary and is disclosed in Ritter. Ritter does not disclose a *plurality* of authorization *modules* executed by a *processor*. Ritter also does not include a processor adapted to determine which type (badge or keyfob) of authorization modules is to be executed by the processor.

Regarding claims 39 and 47, the Examiner argued that Ritter discloses the system of claims 38 and 46, further comprising an authorization-checking device 91 (i.e., a processor) comprising said plurality of authorization modules, wherein said processor processes 91 said fingerprint data received from said user based on an indication of whether said fingerprint data received from said user is authentic in order to permit said user to access an area or a controlled apparatus or process utilizing said access device (citing Ritter col. 4, lines 1-62; col. 5, lines 1-11; FIGS. 1-5).

The Applicant respectfully disagrees with this assessment and notes that the argument presented above against the rejections of independent claims 38 and 46 applies equally against the rejections of dependent claim 39 and 47.

Ritter therefore fails in the aforementioned *prima facie* anticipation test as each and every limitation of the Applicant's claims 38-39 and 46-47 are not disclosed. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §102(e) rejections of claims 38-39 and 46-47 based on the Ritter reference be withdrawn.

III. Claim Rejections - 35 USC § 103

Requirements for Prima Facie Obviousness

The obligation of the examiner to go forward and produce reasoning and evidence in support of obviousness is clearly defined at M.P.E.P. §2142:

> "The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness."

The U.S. Supreme Court ruling of April 30, 2007 (*KSR Int'l v. Teleflex Inc.*) states:

"The TSM test captures a helpful insight: A patent composed of several elements is not proved obvious merely by demonstrating that each element was, independently, known in the prior art. Although common sense directs caution as to a patent application claiming as innovation the combination of two known devices according to their established functions, it can be important to identify a reason that would have prompted a person of ordinary skill in the art to combine the elements as the new invention does."

"To facilitate review, this analysis should be made explicit."

The U.S. Supreme Court ruling states that it is important to identify a *reason* that would have prompted a person to combine the elements and to make that analysis *explicit*. MPEP §2143 sets out the further basic criteria to establish a *prima facie* case of obviousness:

1. a reasonable expectation of success; and
2. the teaching or suggestion of <u>all</u> the claim limitations by the prior art reference (or references when combined).

It follows that in the absence of such a *prima facie* showing of obviousness by the Examiner (assuming there are no objections or other grounds for rejection) and of a *prima facie* showing by the Examiner of a *reason* to combine the references, an applicant is entitled to grant of a patent. Thus, in order to support an obviousness rejection, the Examiner is obliged to produce evidence compelling a conclusion that the basic criterion has been met.

Requirements for Inherency-Based Anticipation

There are a number of factors that must be considered when attempting to establish inherency as a basis for anticipation. Inherency should only be applied under very limited circumstances. That is, inherency permits in very limited circumstances, an invention to be anticipated by prior art that is lacking minor, well-known features in the claimed invention. If the "missing subject matter" is "inherent" or necessarily disclosed in the prior art reference, then anticipation can exist. As stated by the Federal Circuit (see In re Sun USPQ2d 1451, 1453 (Fed. Cir. 1983)

> ...To serve as an anticipation when the reference is silent about the asserted inherent characteristic, such gap in the reference may be filled with recourse to intrinsic evidence. Such evidence must make clear that the missing descriptive matter is necessarily present

in the thing described in the reference and that it would be so recognized by persons of ordinary skill.

In this regard, the CCPA has added that "'[i]nherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient". See In re Oelrich, 666 F.2d 578, 581, 212 USPQ 323, 326 (C.C.P.A. 1981) (quoting Hansgrig v. Kemmer, 102 F.2d 212, 214, 40 USPQ 665, 667 (C.C.P.A. 1930). That is, the missing element or function must necessarily result from the prior art reference.

Additionally, when an Examiner's rejection relies on inherency, it is incumbent upon the Examiner to point to the page and line of the prior art that justifies the rejection based on an inherency theory. The Examiner must not leave the Applicant to guess at the basis of the inherency rejection.

The fact that a certain result or characteristic <u>may</u> occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (reversed rejection because inherency was based on what would result due to optimization of conditions, not what was necessarily present in the prior art); *In re Oelrich*, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.' " *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (citations omitted).

"In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic <u>necessarily</u> flows from the teachings of the applied prior art." *Ex parte Levy,* 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original).

Berardi et al. in view of Ritter

The Examiner rejected claims 26-34 under 35 U.S.C. §103(a) as being unpatentable over Berardi et al. (U.S. Patent Application No. 2003/0167207), hereinafter referred to as "Berardi", in view of Ritter.

Regarding claims 26-34, the Examiner argued that Berardi shows a method for providing access to a financial transaction, where the system includes two versions of the transponder 102. The Examiner admitted that the first embodiment of transponder 102 does not include a fingerprint reader (citing Berardi FIG. 2); the Examiner interpreted this as a badge. The Examiner argued that the second embodiment of transponder 102 includes a fingerprint reader (citing Berardi FIG. 9); the Examiner interpreted this as a keyfob. The Examiner argued that the FIG. 9 transponder sends the fob ID (stored in memory 214) with the fingerprint so both can be authenticated. The Examiner argued that when the data is read from the transponder, a comparison is made to authorize financial access; the Examiner argued that this meets the limitation of determining if the received code is authentic and providing access upon authentication. The Examiner argued that if the data is from a badge, the authorization step compares account data (or the transponder ID), (citing Berardi paragraph [0059]). The Examiner argued that if the data is from a keyfob the authorization step compares fingerprint data, (citing Berardi paragraph [0141]). The Examiner argued that in order to compare the received data from the FIG. 9 transponder with stored fingerprint data, a decision inherently is made that the data received includes fingerprint data. The Examiner stated that this meets the limitation of determining if the code is from a badge or keyfob.

The Examiner admitted that Berardi did not explicitly disclose that the badge and the keyfob utilize the same RF protocol.

The Examiner argued that in the same field of endeavor of dual access communication system, Ritter teaches that an identification data module 40 and a contactless interface 41 utilize the same RF protocol and the same frequency (citing Ritter col. 4, lines 13-19; FIGS. 1-3) in order to automate checking and billing by readers and also identification data can be reproduced by the readers autonomously(?).

The Examiner argued that at the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize using the same RF protocol in the identification data module and an contactless interface for the authorization and checking device taught by Ritter in the RFID reader for interrogating the transponders of Berardi because using the same RF protocol would improve communication with a plurality of access devices autonomously (?) in a access control system.

The Applicant notes that claims 26-31 have been cancelled with this amendment, rendering moot the Examiner's argument against these claims.

Regarding claims 32-34, the Applicant respectfully disagrees with this assessment and notes that independent claim 32 has been amended to include the limitation wherein a processer is *adapted to determine* if said at least one RF signal is derived from said keyfob *or* said badge.

The Examiner has argued that in Berardi a decision is inherently made that the data received includes fingerprint data and therefore this meets the limitation of determining if the code is from a keyfob or a badge. The Applicant submits that there is no *determination* (inherent or not) disclosed in the Berardi reference as to whether the authentication code is of a first or a second type. It is not inherent as Berardi discloses two *non-compatible* embodiments. If one system of Berardi is utilized, then a first type of authentication code is utilized; a second type in the alternate embodiment. Any method disclosed in Berardi does not determine and is incapable of making the determination of whether the authentication code is a first type or a second type. The point is not whether Berardi discloses a first type and a second type as alternative embodiments; the point is whether Berardi discloses the limitation of "*determining*" if there is a first type or a second type. The action of the third step of claim 26 is "determining". The method step of "determining" *must* be disclosed within Berardi in view of Ritter in order for a *prima facie* case of obviousness under 35 U.S.C. §103(a). Berardi in view of Ritter does not disclose this limitation.

Additionally the Examiner argued that in order to compare the received data from the FIG. 9 transponder with stored fingerprint data, a decision inherently is made that the data received includes fingerprint data. The Applicant notes that this is <u>not</u> the Applicant's limitation and is therefore irrelevant. The limitation that the Examiner seems to be arguing is disclosed inherently in Berardi is "analyzing at least one RF signal containing an authentication code to determine whether the authentication code is derived from a keyfob or from a badge". Where is the RF signal analyzed in Berardi? Where is it determined that the signal is from a badge or a keyfob? The Examiner's argument is silent on these limitations.

Furthermore, the Applicant notes that the step in claim 32 which <u>must</u> be disclosed in Berardi in view of Ritter is the step of <u>*analyzing*</u> at least one RF signal containing an authentication code to determine whether the authentication code is derived from a keyfob or from a badge. Berardi in view of Ritter does not disclose (inherent or not) a step of *analyzing* the RF signal to make this determination. The Applicant further notes that claim 32 has been amended to include the limitation wherein a *processer* is *adapted* to determine if said at least one RF signal is derived from said keyfob or said badge. This limitation is disclosed in the Applicant's paragraph [0025] and in FIG. 4 as step 64. The steps of FIG. 4 are performed in a processor adapted to perform these steps, including the step of block 64. In order to disclose this method step, Berardi in view of Ritter must disclose a processor adapted to perform this step as it is not inherent that this step is performed by a processor. Berardi in view of Ritter does not disclose a *processor adapted* to perform this step.

Ritter does not disclose that a keyfob and a badge utilize the same RF protocol, as argued by the Examiner. The Examiner has cited Ritter identification module 40 and the contactless interface 41 as disclosed utilizing the same RF protocol, however, what is actually disclosed in Ritter is that the contactless interface 41 and the authorization-checking device 90 utilize the same RF protocol. This is disclosed in the Examiner's citation in Ritter (col. 4, lines 13-19) as follows:

> Over the contactless interface 41, the external portable authorization-checking device 90 can access the user's identification and authorization data and reproduce these data optically and/or acoustically. The authorization-checking device comprises a housing 91 with a contactless interface using the same protocol and the same frequency as the identification module 40. The housing 91 accommodates the entire electronics (contactless interface, data processing means, battery and/or solar cells, optional additional radio receiver etc.).

The identification module 40 and the contactless interface 41 are part of the same device and do not both transmit. The single identification device of Ritter, which includes both the identification module 40 and the contactless interface 41, is shown in Ritter FIG. 1. This single device of Ritter is equivalent to a keyfob. The authorization-checking device 90 in Ritter is the *receiver* of the authorization system and as such must, of course, utilize the same protocol as the transmitter. This is not the same as the Applicant's claimed invention wherein the *keyfob* and the *badge* utilize the same RF protocol. Ritter, therefore, does not disclose the limitation which the Examiner submits is disclosed.

The Examiner has stated a reason to combine the Berardi and Ritter references as "using the same RF protocol would improve communication with plurality of access device autonomously (?) in an access control system". The Applicant's submits that all that is disclosed in Berardi in view of Ritter is that the *transmitter* and *receivers* in both Berardi and Ritter utilize the same RF protocol and not two different access devices (keyfob and a badge) which utilize the same RF protocol. As the combination does not disclose using the same RF protocol in a keyfob and a badge, what would be a reason to combine the two references?

The Applicant does not understand the Examiner's argument concerning one of ordinary skill in the art. How does using the same RF protocol improve communication with a plurality of access devices _autonomously_? Did the Examiner mean "autonomous access devices" or did the Examiner mean "improves communication *automatically*"? The Applicant respectfully requests a clarification from the Examiner.

The U.S. Supreme Court has stated that an Examiner must provide some *articulated* reasoning with some rationale underpinning to support the legal conclusion of obviousness (KSR opinion, page 14). This articulated reasoning must include a *detailed* explanation of the effects of demands known to the design community or present in the marketplace and the *background knowledge* possessed by a person having ordinary skill in the art. Anything less than such an *explicit* analysis may not be sufficient to support a *prima facie* case of obviousness (KSR opinion, page 14). The Applicant submits that the Examiner has not provided such an explicit reasoning, as required by the U.S. Supreme Court and therefore has not provided a *prima facie* case of obviousness.

Berardi in view of Ritter therefore fails in the aforementioned *prima facie* obviousness test as each and every limitation of the Applicant's claim 32-34 is not disclosed. Furthermore, the Examiner has not provided an *explicit* reason, as required by the U.S. Supreme Court, to combine the Berardi and Ritter references. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §103(a) rejections of claims 32-34 based on Berardi in view of Ritter be withdrawn.

Berardi in view of Ritter/Fitzgibbon

The Examiner rejected claims 1-7, 9-16, 19-21, 23-35 and 35-36 under 35 U.S.C. §103(a) as being unpatentable over Berardi in view of Ritter and in further view of Fitzgibbon et al. (U.S. Patent Application No. 2003/0210131), hereinafter referred to as "Fitzgibbon".

Regarding claims 1-6, the Examiner argued that Berardi shows a method for providing access to a financial transaction, where the system includes two versions of the transponder 102. The Examiner argued that the first embodiment of transponder 102 does not include a fingerprint reader (citing Berardi FIG. 2); the Examiner interpreted this as a badge. The Examiner argued that the second embodiment of transponder 102 includes a fingerprint reader (citing Berardi FIG. 9); the Examiner interpreted this as a keyfob. The Examiner argued that the FIG. 9 transponder sends the fob ID (stored in memory 214) with the fingerprint so both can be authenticated. The Examiner argued that when the data is read from the transponder, a comparison is made to authorize financial access; the Examiner stated that this meets the limitation of determining if the received code is authentic and providing access upon authentication. The Examiner argued that if the data is from a badge, the authorization step compares account data (or the transponder ID citing Berardi paragraph [0059]). The Examiner argued that if the data is from a keyfob, the authorization step compares fingerprint data (citing Berardi paragraph [0141]). The Examiner argued that in order to compare the received data from the FIG. 9 transponder with stored fingerprint data, a decision inherently is made that the data received includes fingerprint data. The Examiner stated that this meets the limitation of determining if the code is from a badge or keyfob.

The Examiner admitted that Berardi did not explicitly disclose that the badge and the keyfob utilize the same RF protocol and wherein the authentication code from the fingerprint keyfob comprises a digitized fingerprint signature and a rolling identifier.

The Examiner argued that in the same field of endeavor of dual access communication system, Ritter teaches that an identification data module 40 and a contactless interface 41 utilize the same RF protocol and the same frequency (citing Ritter col. 4, lines 13-19; FIGS. 1-3) in order to automate checking and billing by readers and also identification data can be reproduced by the readers autonomously(?).

The Examiner argued that at the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize using the same RF protocol in the identification data module and an contactless interface for the authorization and checking device taught by Ritter in the RFID reader for interrogating the transponders of Berardi because using the same RF protocol would improve communication with a plurality of access devices autonomously (?) in a access control system.

The Examiner argued in an analogous art, Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for access authorization. The Examiner argued that the portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. The Examiner argued that Fitzgibbon includes a processor (citing Fitzgibbon FIG. 4) in communication with the transmitters to process data received and make an authorization determination, (citing Fitzgibbon FIG. 8). The Examiner argued that Fitzgibbon teaches that in this type of system, the use of rolling codes can improve the security of the system. The Examiner argued that the fingerprints and rolling codes are separately checked against databases for authenticity, (citing Fitzgibbon FIG. 8).

The Examiner argued that therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have used the fingerprint and rolling code processing of Fitzgibbon in the fingerprint entry transponder embodiment of Berardi in view of Ritter because adding rolling code authentication increases security in the system.

The Applicant respectfully disagrees with this assessment and notes that claim 1 has been amended to include the limitation of a processor which is adapted to determine whether the received authentication code is from the badge or the fingerprint keyfob. The argument presented above against the rejections of claims 32-34 applies equally against the rejections against claims 1-6 as both sets of claims include the same amended limitation. Berardi in view of Ritter does not disclose a *processor adapted* to perform this step of determining whether the received authentication is from a badge or a fingerprint keyfob.

The Applicant furthermore submits that the Examiner has not provided an explicit reasoning to combine the Berardi, Ritter and Fitzgibbon references as argued above.

Berardi in view of Ritter and further in view of Fitzgibbon therefore fails in the aforementioned *prima facie* obviousness test as each and every limitation of the Applicant's claim 1-6 is not disclosed. Furthermore, the Examiner has not provided an *explicit* reason, as required by the U.S. Supreme Court, to combine the Berardi, Ritter and Fitzgibbon references. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §103(a) rejections of claims 1-6 based on Berardi in view of Ritter and further in view of Fitzgibbon be withdrawn.

Regarding claims 7, 9-16, 18-21 and 23-25, the Examiner argued that Berardi shows a method for providing access to a financial transaction, where the system includes two versions of the transponder 102. The Examiner argued that the first embodiment of transponder 102 does not include a fingerprint reader (citing Berardi FIG. 2); the Examiner interprets this as a badge. The Examiner argued that the second embodiment of transponder 102 includes a fingerprint reader (citing Berardi FIG. 9); the Examiner interprets this as a keyfob. The Examiner argued that the FIG. 9 transponder sends the fob ID (stored in memory 214) with the fingerprint so both can be authenticated. The Examiner argued that when the data is read from the transponder, a comparison is made to authorize financial access; this meets the limitation of determining if the received code is authentic and providing access upon authentication, the Examiner argued. The Examiner argued that if the data is from a badge, the authorization step compares account data (or the transponder ID), (citing Berardi paragraph [0059]). The Examiner argued that if the data is from a keyfob the authorization step compares fingerprint data, (citing Berardi paragraph [0141]). The Examiner argued that in order to compare the received data from the FIG. 9 transponder with stored fingerprint data, a decision inherently is made that the data received includes fingerprint data. The Examiner stated that this meets the limitation of determining if the code is from a badge or keyfob.

The Examiner admitted that however, Berardi does not explicitly disclose that the badge and the keyfob utilize the same RF protocol and wherein the authentication code from fingerprint keyfob comprises a digitized fingerprint signature and a rolling identifier and wherein the authentication code from the keyfob comprises first and second portions, wherein the first and second portions are different types of codes.

The Examiner argued that in the same field of endeavor of dual access communication system, Ritter teaches that an identification data module 40 and an contactless interface 41 utilize the same RF protocol and the same frequency (citing Ritter col. 4, lines 13-19; citing FIGS. 1-3) and wherein the authentication code from the terminal 4 comprises identification data (i.e., first) and authorization data (i.e., second portions), wherein the first and second portions are different types of codes (citing Ritter col. 5, lines 29-37; citing FIGS. 1-3) in order to automatic checking and billing by readers and also identification data can be reproduced by the readers autonomously.

The Examiner argued that at the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize using the RF protocol in the identification data module and an contactless interface for the authorization and checking device taught by Ritter in the RFID reader for interrogating the transponders of Berardi because using the same RF protocol would improve communication with plurality of access device autonomously in a access control system.

The Examiner argued that in an analogous art, Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for access authorization. The Examiner argued that the portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. The Examiner argued that Fitzgibbon includes a processor (citing Fitzgibbon FIG. 4) in communication with the transmitters to process data received and make an authorization determination, (citing Fitzgibbon FIG. 8). The Examiner argued that Fitzgibbon is cited for teaching that in this type of system, the use of rolling codes can improve the security of the system. The Examiner argued that the fingerprints and rolling codes are separately checked against data bases for authenticity (citing Fitzgibbon FIG. 8).

The Examiner argued that therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have used the fingerprint and rolling code processing of Fitzgibbon in the fingerprint entry transponder embodiment of Berardi in view of Ritter because adding rolling code authentication increases security in the system.

Regarding claims 35-36, the Examiner argued that Berardi in view of Ritter and in further view of Fitzgibbon disclose the method of claim 32, Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for access authorization. The Examiner argued that the portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. The Examiner argued that Fitzgibbon includes a processor (citing Fitzgibbon FIG. 4) in communication with the transmitters to process data received and make an authorization determination, (citing Fitzgibbon FIG. 8). The Examiner argued that Fitzgibbon is cited for teaching that in this type of system, the use of rolling codes can improve the security of the system. The Examiner argued that the fingerprints and rolling codes are separately checked against databases for authenticity (citing Fitzgibbon FIG. 8).

The Applicant respectfully disagrees with this assessment and notes that claim 7 and 14 have been amended to include the limitation of a processor which <u>is adapted to determine</u> whether the received authentication code is from the badge or the fingerprint keyfob. The argument presented above against the rejections of claims 32-34 applies equally against the rejections against claims 7, 9-16, 18-21, 23-25 and 35-36 as both sets of claims include the same amended limitation. Berardi in view of Ritter does not disclose a *processor adapted* to perform this step of determining whether the received authentication is from a badge or a fingerprint keyfob.

The Applicant furthermore submits that the Examiner has not provided an explicit reasoning to combine the Berardi, Ritter and Fitzgibbon references as argued above.

Berardi in view of Ritter and further in view of Fitzgibbon therefore fails in the aforementioned *prima facie* obviousness test as each and every limitation of the Applicant's claim 7, 9-16, 18-21, 23-25 and 35-36 is not disclosed. Furthermore, the Examiner has not provided an *explicit* reason, as required by the U.S. Supreme Court, to combine the Berardi, Ritter and Fitzgibbon references. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §103(a) rejections of claims 7, 9-16, 18-21, 23-25 and 35-36 based on Berardi in view of Ritter and further in view of Fitzgibbon be withdrawn.

Ritter in view of Usui

The Examiner rejected claims 40-44 and 48-52 under 35 U.S.C. § 103(a) as being unpatentable over Ritter in view of Usui (U.S. Patent No. 7,242,276).

Regarding claims 40-41 and 48-49, the Examiner argued that Ritter discloses the method of claim 38 and 46, however, the Examiner admitted that Ritter did not explicitly disclose that wherein said access device comprises a door lock and wherein said door lock comprises a stand alone push button lock that utilizes an authentication code to activate said stand alone push button lock, wherein said authentication code is changeable utilizing said processor.

The Examiner argued that in the same field of endeavor of access control system, Usui discloses a door lock system (1) (citing Usui col. 2, lines 16-26; FIG 1) and wherein said door lock (1) comprises a stand alone push button lock that utilizes an authentication code is changeable utilizing said control unit 30 (i.e., processor) (citing Usui col. 2, lines 27-62; FIG. 1-3) in order to improve security of a doorway locking system.

The Examiner argued that at the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize applying the door lock system with authentication code to activate the lock taught by Usui in the RFID reader for interrogating the transponders for checking the authorization of users of Ritter because using authentication code to activate the door lock would improve a plurality of utility of the access control system.

Regarding claims 42-43 and 5-51, the Examiner argued that Ritter discloses the method of claim 38 and 46, and Usui discloses a fingerprint keyfob reader (citing Usui col. 2, lines 39-46; FIGS 2 and 3).

Regarding claims 44 and 52, the Examiner argued that Ritter discloses the method of claim 38 and 46, and Usui discloses a fingerprint keyfob reader (citing Usui col. 2, lines 39-46; citing FIGS. 2 and 3), the Examiner argued that it would be obvious to replace the finger print reader with a magnetic strip reader because the magnetic stripe reader is a conventional reader.

The Applicant respectfully disagrees with this assessment and notes that the argument presented above against the rejections of claims 38-39 and 46-47 over Ritter applies equally against the rejections of claims 40-41 and 48-52 as independent claims 38 and 46 include the limitation wherein a processor is adapted to determine which of said plurality of authorization modules is to be executed by said processor. As submitted above, Ritter does not disclose this limitation and this limitation is not disclosed in Usui.

Furthermore, the Applicant submits that the Examiner has not provided an *explicit* reasoning why one of ordinary skill in the art would combine the references, as argued above. The Applicant notes that the Examiner's argument concerning one of ordinary skill in the art is not understood. What is "a plurality of utility of the access system" and how does one improve it? The Applicant respectfully requests clarification.

Additionally, the Applicant notes that the limitations of claims 42 and 44 are wherein at least on of the plurality of authorization modules comprises a keyfob reader (claim 42) and a magnetic stripe reader (claim 44); however, the Examiner has cited Ritter FIG. 1 (identification module 40 and a contactless interface 41) as disclosing the plurality of authorization modules. As submitted above, identification module 40 and contactless interface 41 are components of the same *badge*. If these components disclosed in Ritter are the plurality of authorization modules, as the Examiner asserts, how can a badge possibly comprise a badge reader? Combining Ritter with Usui in this case would not make sense as the badge would also be the very component that would be necessary to read the badge itself. This combination would fail as a secure access system. Therefore, Ritter in view of Usui would <u>not</u> result in a functioning security system and therefore teaches <u>*away*</u> from the combination.

Ritter in view of Usui therefore fails in the aforementioned *prima facie* obviousness test as each and every limitation of the Applicant's claim is not disclosed. The Examiner has not provided an articulated rationale why one of ordinary skill in the art one would combine the Ritter and Usui references. Additionally, Ritter in view of Usui teaches away from the combination.

Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §103(a) rejections of claims 40-44 and 48-52 based on Ritter in view of Usui be withdrawn.

Ritter in view of Fitzgibbon

The Examiner rejected claims 45 and 53 under 35 U.S.C. § 103(a) as being unpatentable over Ritter in view of Fitzgibbon.

Regarding claims 45 and 53, the Examiner argued that Ritter discloses the method of claim 38 and 46, however, the Examiner admitted that Ritter did not explicitly disclose wherein said data is generated by said at least one of said plurality of authorization modules based on a shared and indexed mathematical function that prevents authorizing of said data, if said data is not authorized based on a particular sequence with respect to said shared and indexed mathematical function.

The Examiner argued that in the same field of endeavor of access control system, Fitzgibbon discloses learning a rolling code and storing in an associated table via an address of the table, looking up in the code table is considered a shared and indexed mathematical function as claimed (citing Fitzgibbon paragraph [0052]; citing FIG. 5) in order to improve security in an access control system.

The Examiner argued that at the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize using a rolling code and storing in an associated table as taught by Fitzgibbon in the RFID reader for interrogating the transponders and for checking the authorization of users of Ritter because using rolling code and storing in an associated table would improve security in communication of the access control authorization system.

The Applicant respectfully disagrees with this assessment and notes that the argument presented above against the rejections of claims 38-39 and 46-47 over Ritter applies equally against the rejections of claims 45 and 53 as independent claims 38 and 46 include the limitation wherein a processor is adapted to determine which of said plurality of authorization modules is to be executed by said processor. As submitted above, Ritter does not disclose this limitation and this limitation is not disclosed in Fitzgibbon.

Ritter in view of Fitzgibbon fails in the aforementioned prima facie obviousness test as each and every limitation of the Applicant's claims is not disclosed. Furthermore, the Examiner has not provided an explicit rationale as to why one of ordinary skill in the art would combine the Ritter and Fitzgibbon references, as submitted above. Based on the foregoing, the Applicant respectfully requests that the 35 U.S.C. §103(a) rejections of claims 45 and 53 based on Ritter in view of Fitzgibbon be withdrawn.

IV. Conclusion

In view of the foregoing discussion, the Applicant has responded to each and every rejection of the Official Action. The Applicant has clarified the structural distinctions of the present invention. Applicant respectfully requests the withdrawal of the rejections under 35 U.S.C. §102 and 35 U.S.C. §103 based on the preceding remarks. Reconsideration and allowance of Applicant's application is also respectfully solicited.

Should there be any outstanding matters that need to be resolved, the Examiner is respectfully requested to contact the undersigned representative to conduct an interview in an effort to expedite prosecution in connection with the present application.

Respectfully submitted,

Kermit Lopez

Dated: June 20, 2008

Kermit Lopez
Attorney for Applicants
Registration No. 41,953
ORTIZ & LOPEZ, PLLC
P.O. Box 4484
Albuquerque, NM 87196-4484
505-314-1312